2/PRTS

INTEGRATED SOFTWARE AND METHOD FOR AUTHENTICATING SAME

DESCRIPTION

BACKGROUND OF THE INVENTION

The invention relates to integrated software and a method of authenticating the latter, in particular in the field of digital television decoders.

DESCRIPTION OF THE PRIOR ART

In the devices of the prior art, an integrity test of integrated software is normally performed by computing, using an external tool, a reference signature of this software representative of the latter and by inserting the latter into this software. During the software initialization phase, the software computes its own signature and compares this signature with the reference signature. If these signatures are different, the software executes a software routine specific to a defense procedure, otherwise it continues normally.

In the case of an authentication of such software, it is desirable to check the source of the latter. A known solution consists in applying the principle of the integrity test and combining it with an asymmetrical cryptographic algorithm: the reference signature is encrypted with a private key and the result is integrated, in the form of a certificate, in the software. During the checking phase, the reference signature is decrypted with a public key incorporated in the software before being compared to the reference signature.

A first document of the prior art, ETSI standard TS 101 812 V1-1-1 entitled "Digital Video Broadcasting (DVB) Multimedia Home Platform (MHP) Specification 1.0" (2000-07), in particular sections 12.2 and 12.7, describes the implementation of a method of authenticating software downloaded into a terminal by carrying out an authentication by certificate of said downloaded software by means of software integrated in said terminal.

A second document of the prior art, US 6,167,521, describes a method of downloading new software into a system, the purpose of which is to prevent this new downloaded software from attacking software already installed in this system, or, conversely, to prevent the software already installed from attacking the new software, in particular when the respective software owners do not have confidence in each other.

More specifically, to perform a software authentication, the use of software contained in a memory in a first fixed, that is, write-protected, part 10 to authenticate application software of a second part 11, which may have been downloaded, using a certificate 12 located in this second part 11, is known, as illustrated in figure 1.

Thus, in the decoder field, when a customer seeks out the service provider with new application software, the latter provides him with software for verifying this application software and a certificate to be associated with said application software.

However, in such a solution, there is no way for the provider of the first software to check that the authentication procedure has indeed taken place.

The object of the invention is to enable the provider to check that this authentication has indeed taken place and that his rights have therefore indeed been respected by the customer.

SUMMARY OF THE INVENTION

The present invention therefore proposes a method for authenticating software downloaded in a terminal, said method comprising a step for authenticating by certificate said downloaded software by means of software integrated in said terminal, characterized in that it also comprises a step for authenticating by certificate, during execution of said downloaded software, said first integrated software by means of an authentication software module associated with said downloaded software.

Advantageously, the first integrated software authenticates the downloaded software by means of an authentication library and a first certificate; the first integrated software and the authentication library form a first part of write-protected memory, the downloaded software and this first certificate form a second part of loadable memory.

Advantageously, the first part also includes a second certificate, the second part also includes verification software, and, once the downloaded software has been authenticated, the verification software authenticates the first software by means of the authentication library and the second certificate.

Advantageously, these two successive authentications take place on initialization. The second part can be downloaded.

The invention also relates to integrated software comprising a first write-protected memory part formed from first software and an authentication library, and a second part including application software and a first certificate, characterized in that the first part also includes a second certificate, and in that the second part also includes verification software.

This software can be used, for example, in a digital television decoder, in a PC (personal computer) type terminal, or in any other integrated device.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates an authentication method of the prior art.

Figure 2 illustrates the authentication method of the invention.

Figure 3 illustrates an example of a certificate.

Figure 4 illustrates an example of signature.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the method of the invention, as in the method of the prior art illustrated in figure 1, first software contained in a first part 10 of write-protected memory authenticates, for example in the initialization phase, second software, which is the application software, located in a second loadable part 11 using an authentication library located in the first part and a certificate 12 located in this second part 11.

Since the term "certificate" has a quite particular meaning (an electronic identity which is issued by a trusted third party for a person or a network entity, each certificate being signed with the private signature key of a certification authority) and is too limiting in the authentication techniques, the term "certificate" used in the present description is meant to cover also, more generally, the terms signature, CRC or other data required to verify the authenticity/integrity of software.

In the method of the invention, the first part 10 also includes a second certificate 13, as illustrated in figure 2. The second part 11 also includes verification software. This verification software, once the application software has been authenticated, authenticates the first software by means of the authentication library and the second certificate.

Such a method enables the supplier of the first software to check that the customer using the application software does indeed respect his rights.

In an exemplary embodiment, the format of the certificate, illustrated in figure 3, is as follows:

- Header:
  - CLP ("Certificate Location Pattern"): pattern giving the location of the certificate to find the authentication certificate in the memory (for example, 8 bytes),
  - RFU ("Reserved for Future Use"): reserved for a future use (for example 1 byte),
  - K: key number to be used (for example, 1 byte),
- Signature (for example, 128 bytes) which is the result of an RSA encryption, with a private key, of 1024 bits of the message illustrated in figure 4.

The 1024-bit signature begins with a byte at 0 to enable its RSA encryption, the rest 20 is filled randomly in a different way before each encryption.

At the offset H_CODE_OFFSET from the start of the message, there is a hash code SHA1 on 20 bytes. This H_CODE is preceded by a CHECK_PATTERN pattern, the function of which is to enable distinction between a wrong decryption (public key number or value, algorithm, inconsistent certificate) and a wrong H_CODE during the integrity check.